



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,133	08/10/2001	Russell Andrew Fink	00-4045	6468

32127 7590 04/28/2006

VERIZON CORPORATE SERVICES GROUP INC.  
C/O CHRISTIAN R. ANDERSEN  
600 HIDDEN RIDGE DRIVE  
MAILCODE HQEO3H14  
IRVING, TX 75038

EXAMINER

TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 04/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/928,133

Applicant(s)

FINK ET AL.

Examiner

Tamara Teslovich

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 February 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

This office action is in response to Applicant's request for continued examination filed February 9, 2006.

Claims 1, 4, 6, 9, 11, 14, 16, and 19 are amended.

Claims 1-24 are herein considered.

#### ***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 9, 2006 has been entered.

***Response to Arguments***

Applicant's arguments concerning the Examiner's 35 U.S.C. 102(b) and 35 U.S.C. 103(a) rejection of claims 1-24 as being anticipated by **Deng** et al. (U.S. Patent No. 6,701,432 B1) have been fully considered and are persuasive.

Applicant's arguments concerning the Examiner's 35 U.S.C. 102(b) rejection of claims 1-24 as being anticipated by **Kraemer** et al. (U.S. Patent No. 5,798,706) have been fully considered but they are not persuasive.

In response to the Applicant's first set of arguments concerning Kraemer and its alleged failure to suggest issuing a request to the network to resolve the address in response to detecting a source address or destination address that does not match an entry in one of the tables the Examiner respectfully disagrees. Column 4, specifically lines 33-67, disclose the use of RARP as well as ARP protocols and servers in order to resolve addresses in response to a failure to find the addresses within the local entry tables. Lines 51-52 teach that an ARP protocol be utilized in order to dynamically build the local tables, adding in new addresses as they are validated. With Kraemer's suggestion of 'dynamically built tables' it is clear that those tables are revised and updated as information becomes available. The Applicant specifically argues that the Kraemer patent fails to teach or suggest issuing a request to the network, be it an ARP request or otherwise, to resolve an address when the address does not match an entry in the host table. At this point the Examiner would like to refer back to column 4, specifically lines 51-52 in which the table is built dynamically using an ARP protocol on

IP addresses. The Examiner would like to bring to the Applicant's attention that the utilization of the ARP, by definition, includes broadcasting an ARP packet containing the Internet address of a host and waiting for that host (or some other host) to send back a response including an Ethernet address. Therefore, Kraemer's teaching of a dynamic table utilizing the Address Resolution Protocol (ARP) teaches issuing a request, an ARP packet to the network to resolve a network address for those addresses that do not already appear in the table. The Applicant goes on to argue that Kraemer fails to teach or suggest supplementing the host table with the address upon receiving a reply to the request that indicates the address is valid. As explained above, the dynamic table disclosed by Kraemer utilizes ARP for those addresses not included within it, and by sending out ARP requests and receiving responses thereto, dynamically updates the table.

The Applicant's arguments concerning independent claims 6, 11, and 16 rely upon those arguments given with respect to claim 1 above and are rejected for the same reasons. All dependent claims remain rejected as well.

Therefore, based on the above arguments, the Examiner maintains the rejections as set forth below.

### ***Claim Rejections - 35 USC § 102***

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

**Claims 1-24 are rejected under 35 U.S.C. 102(b) as being anticipated by Kraemer et al. (U.S. Patent No. 5,798,706).**

As per **Claim 1**, Kraemer et al. discloses an apparatus for detecting adversarial activity on a network, comprising a memory adapted to store a host table (see col.3 lines 46-60); a key exchanger adapted to derive a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"); a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); a mapping device adapted to map the address to the host table (see col.3 line 60 thru col.4 line 2); a host resolution device adapted to issue a request to the network to resolve the address when the address does not match an entry in the host table and to supplement the host table with the address upon receipt of a reply to the request that indicates that the address is valid (col.4 lines 33-52); and an actuator adapted to trigger a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per **Claim 2**, Kraemer et al. discloses an apparatus as set forth in Claim 1, wherein the security device is a logging device adapted to log the data packet (see col.4 lines 3-5 and 26-31).

As per **Claim 3**, Kraemer et al. discloses an apparatus as set forth in Claim 1, wherein the security device is adapted to signal an alarm when triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim 4**, Kraemer et al. discloses an apparatus as set forth in Claim 1, further comprising a host resolution device adapted to derive the host table using an address resolution protocol (see col.4 lines 48-52).

As per **Claim 5**, Kraemer et al. discloses an apparatus as set forth in Claim 1, further comprising a network device adapted to place the data packet onto a network when the address maps to the host table (col.1 line 66 through col.2 line 9 and col.2 lines 27-31).

As per **Claim 6**, Kraemer et al. discloses a method for detecting adversarial activity on network, comprising storing a host table (see col.3 lines 46-60); deriving a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"); translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); mapping the address the host table (see col.3 line 60 thru col.4 line 2); issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid

(col.4 lines 33-52); and triggering a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per **Claim 7**, Kraemer et al. discloses a method as set forth in Claim 6, further comprising logging the data packet when the address does not match an entry in the host table (see col.4 lines 3-5 and 26-31).

As per **Claim 8**, Kraemer et al. discloses a method as set forth in Claim 6, further comprising signaling an alarm when the security device is triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim 9**, Kraemer et al. discloses a method as set forth in Claim 6, further comprising deriving the host table using an address resolution protocol (see col.4 lines 48-52).

As per **Claim 10**, Kraemer et al. discloses a method as set forth in Claim 6, further comprising placing the data packet onto a network when the address maps to the host table (see col.4 lines 3-5 and 26-31).

As per **Claim 11**, Kraemer et al. discloses a device for detecting adversarial activity on a network, comprising means for storing a host table (see col.3 lines 46-60); means for deriving a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"); means for translating predetermined portions of header information of a data packet according to a packet cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); means



for mapping the address to the host table (see col.3 line 60 thru col.4 line 2); means for issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid (col.4 lines 33-52); and means for triggering a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per **Claim 12**, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for logging the data packet when the address does not match an entry in the host table (see col.4 lines 3-5 and 26-31).

As per **Claim 13**, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for signaling an alarm when the security device is triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim 14**, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for deriving the host table using an address resolution protocol (see col.4 lines 48-52).

As per **Claim 15**, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for placing the data packet network when the address maps to the host table (see col.4 lines 3-5 and 26-31).

As per **Claim 16**, Kramer et al. discloses a bastion host adapted for processing packet header information of a data packet, the bastion host being operable to store a host table (see col.3 lines 46-60) derive a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN");

translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); map the address to the host table (see col.3 line 60 thru col.4 line 2); issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid (col.4 lines 33-52); and trigger a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per **Claim 17**, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to log the data packet when the address does not match an entry in the host table (see col.4 lines 3-5 and 26-31).

As per **Claim 18**, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to signal an alarm when the security device is triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per **Claim 19**, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to derive the host table using an address resolution protocol (see col.4 lines 48-52).

As per **Claim 20**, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to place the data packet onto a network when the address maps to the host table (see col.4 lines 3-5 and 26-31).

As per **Claim 21**, Kraemer et al. discloses the apparatus as set forth in Claim 1, wherein said key exchanger is further adapted to repeatedly derive a cipher key with the cipher key derived by said key exchanger over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

As per **Claim 22**, Kraemer et al. discloses the method as set forth in Claim 6, wherein deriving the cipher key comprises repeatedly deriving a cipher key such that the resulting cipher key changes over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

As per **Claim 23**, Kraemer et al. discloses the device as set forth in Claim 11, wherein said means for deriving a cipher key is further adapted to repeatedly derive a cipher key such that the resulting cipher key changes over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

As per **Claim 24**, Kraemer et al. discloses the bastion host as set forth in Claim 16, wherein said the bastion host is further operable to repeatedly derive a cipher key such that the resulting cipher key changes over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
TT/ELM

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER